拡張Lorenz写像に基づく擬似乱数のデジタルハードウェア化の研究

修士学位論文要約（令和２年３月）

拡張 Lorenz 写像に基づく擬似乱数のデジタルハードウェア化の研究

宮内　清孝
指導教員：堀尾 喜彦

Digital Hardware Implementation of Pseudorandom Number Generator Based on Augmented Lorenz Map

Kiyotaka MIYAUCHI
Supervisor: Yoshihiko HORIO

A chaos-based stream cipher using an augmented Lorenz map has been proposed. It was shown through numerical simulations that this chaotic map can generate statistically secure pseudorandom numbers, although high-speed hardware is necessary for practical use. In this paper, we experimentally demonstrate through field programmable gate array (FPGA) prototyping, high-speed and small-sized digital hardware implementation of the pseudorandom number generator based on the augmented Lorenz map. In particular, we examine the effect of reduction of the size of the look-up table (LUT) for the sine function, and of bit length for calculations, on the performance of the resulting pseudorandom number.

1. はじめに

近年の情報技術の発展に伴い、エッジデバイスが増加することで、ネットワークを介する情報量が増大し、セキュリティ問題がますます重要となっている。そのため、エッジデバイスに搭載するための高速・小型・低消費電力で安全性の高い暗号用ハードウェアが必要とされている。その候補として、拡張 Lorenz 写像を用いたカオスストリーム暗号がある [1]。この方法では、カオスの複雑な挙動に基づき、乱数を生成している。しかしながら、その生成速度は、既存の暗号と比較して劣っているため、高速化が必要である。そこで本論文では、拡張 Lorenz 写像に基づく擬似乱数生成をデジタルハードウェア化するための検討を行う。その際、高い安全性を保ちつつ、高速化と小型化を目指す。

2. 拡張 Lorenz 写像に基づくカオス暗号

拡張 Lorenz 写像は、従来のカオス暗号の欠点である鍵空間等の問題を解決した手法として提案された。拡張 Lorenz 写像は以下のように表される。

$$y_{i+1} = \sum_{n=1}^{N} \frac{x_{n,i}}{M_n^2} \qquad (2.1)$$

$$x_{n,i+1} = x_{n,i} y_i - z_{n,i} \qquad (2.2)$$

$$z_{n,i+1} = \sin(w_n y_i) \qquad (2.3)$$

$$w_n = R\sin(M_n \varphi) \qquad (2.4)$$

$$M_n = n + \varepsilon Q_{n-1} \qquad (2.5)$$

ここで、$x_{n,i}, y_i, z_{n,i}$ は総数 $2N$+1 個の変数、i は離散時間ステップ、n は 1 から N までの整数、ε は正の微小定数、R、φ は分岐パラメータ、Q_{n-1} は秘密鍵を表す 2 進乱数列、M_n は Q_{n-1} から得られる値で、$Q_0 = 0, M_1 = 1$ である。

拡張 Lorenz 写像は、式(2.1)の変数 y_i を中心ノードとし、N 個のサブシステムが星型ネットワーク状に結合した $2N$+1 次元のカオス動力学モデルである。N の値はサブシステムの個数により任意に設定できるため、N を変化させることにより、秘密鍵の取り得る個数 2^{N-1} を任意に変更することができる。この特長により、今後求められる鍵長が増加した場合にも、柔軟に対応できる。

3. デジタルハードウェア化の検討

拡張 Lorenz 写像のハードウェア化にはいくつかの問題点がある。まず、拡張 Lorenz 写像がカオス動力学モデルであることから、本来無限ビット長の精度が必要とされる。しかし、アナログハードウェア実装の場合では、ノイズにより同じ初期条件から計算しても全く異なる時系列が出力されるため、暗号には不向きである。よって、物理的なノイズの影響が無いデジタルハードウェアによる実装を考える。

デジタルハードウェア実装の場合には、計算精度の問題が生じる。より高速に動作させるためには、ビット長を短くすることが考えられるが、この場合、量子化誤差により本来のカオスとは異なる計算となり、生成される擬似乱数の性能が低下する可能性がある。また別の方法としては、ルックアップテーブル(LUT)などを用いて計算を単純化する方法もあるが、この場合にも、近似誤差などの影響により本来の拡張 Lorenz 写像の計算と異なるため、性能が低下する可

能性がある。従って、上記の問題点を考慮し、生成される擬似乱数の性能を保ちつつ、ハードウェア性能を向上させる方法を検討する必要がある。

これまで、擬似乱数生成ハードウェアの高速化、小型化のため、sin 関数の実装方法 [2]や計算ビット長削減 [3]の検討を行ってきた。sin 関数の実装には、一般に高速実装可能な LUT を用い、その際に生じる近似誤差を考慮しつつ、LUT の小型化を行った。計算ビット長を削減する際には、量子化誤差の影響を考慮し、擬似乱数の性能が保たれる最も短いビット長を探索した。

4. FPGA を用いたデジタルハードウェア実装

本章では、Field Programmable Gate Array (FPGA)を用いて、ハードウェア性能を評価する。FPGA は再構成可能なデジタルハードウェアシステムであり、短時間で多くのアーキテクチャを評価できる利点がある。本研究では、Xilinx 社の VCU118 評価ボードと Vivado2018.3 を使用した。

計算には固定小数点演算を使用し、擬似乱数は変数 $x_{n,i}$ の最下位ビットを取り出して生成する。擬似乱数の評価には、NIST SP800-22[4]を用いた。この検定は、擬似乱数の予測不可能性や無作為性等の性質を保証するために一般的に使用されている。ハードウェアの評価には、擬似乱数生成速度とハードウェアサイズを使用した。ここで、ハードウェアサイズは Vivado2018.3 で報告される FPGA 内のフリップフロップと LUT の使用数の和とする。

図 1 は、LUT の分割数と小数部ビット長を変化させた場合のハードウェア性能を示した図である [5]。横軸は、実装した LUT の分割数と小数部ビット長の組み合わせを表す。なお、図には NIST 検定に合格した擬似乱数を生成した実装のみを示している。図 1 より、小数部が 24 ビット、LUT の分割数が 890 の場合に最も良い性能であることがわかる。ただし、擬似乱数生成速度が最も高速だったのは、小数部が 24 ビット、LUT の分割数が 1024 の場合である。

表 1 に実装方法による性能比較の結果を示す。実

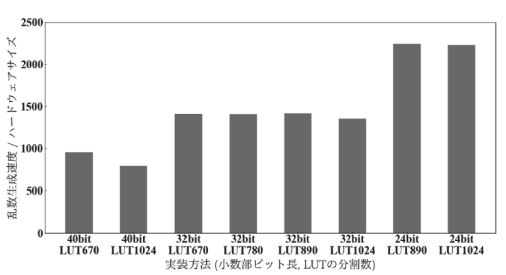

図 1　LUT の分割数と小数部ビット長を変化させた場合のハードウェア性能。

表 1　実装方法による性能比較。

	速度 [Mbps]	サイズ
I. 先行文献値 [1] 64bit 浮動小数点 シミュレーション	33.3 : 1 倍	---
II. 64bit 浮動小数点 [5] 5 次 Taylor 展開	171.2 : 5.2 倍	331436 : 1 倍
III. 24bit, LUT890[5] サイズ最小	387.2 : 11.63 倍	172682 : 0.521 倍
IV. 24bit, LUT1024[5] 速度最大	388.7 : 11.67 倍	174624 : 0.527 倍

装 I は 64 ビット浮動小数点演算を用いてソフトウェア実装した先行文献 1)における値であり、実装 II、III、IV は FPGA によるハードウェア実装の値である。表 1 より、速度が最大になった実装 IV は、先行文献値の 11.67 倍となる高速化を達成している。また、サイズが最小となった実装 III は、実装 II の 0.521 倍の小型化を達成している。

また、小数部ビット長削減の過程で、あるビット長で一度検定に不合格になっても、さらにビット長を短くすると、検定に合格する場合があることを発見した [3]。このことは、ビット長が短くなることで量子化誤差が増大し、生成される擬似乱数の性能が悪化するという直感に反した結果である。これは、適当な量子化誤差が拡張 Lorenz 写像のカオスダイナミクスと協調することで、全体として複雑性を保つため、擬似乱数の性能が保たれているのではないかと考えられる。

5. まとめ

拡張 Lorenz 写像に基づくストリーム暗号のデジタルハードウェア化について検討した。LUT の小型化や小数部ビット長を短くすることで、ハードウェアの高速化と小型化が達成できることを示した。今後は、更なる高速化、小型化のため、演算器を拡張 Lorenz 写像に適した実装に最適化することや、擬似乱数の更なる安全性の保証のため TestU01 BigCrush テストを行うことなどが挙げられる。また、カオスと量子化誤差の相互作用についてもさらに深く検討する必要がある。

文献

1) 長憲一郎, 宮野尚哉, 信学論, J101-A(8), 2018.
2) 宮内清孝 他, 信学総大, N-1-31, p. 279, 2019.
3) 宮内清孝 他, 信学ソ大, N-1-2, p. 147, 2019.
4) A. Ruklin *et al.*, NIST Special Publication 800-22 Revision 1a (Revised April 2010).
5) K. Miyauchi *et al.*, NOLTA, IEICE, 2020, submitted.